

(51) 国際特許分類6

G06K 19/073, G07B 15/00

A1

(11) 国際公開番号

WO98/36377

(43) 国際公開日

1998年8月20日(20.08.98)

(21) 国際出願番号

PCT/JP98/00512

(22) 国際出願日

1998年2月6日(06.02.98)

(30) 優先権データ

特願平9/28859

1997年2月13日(13.02.97)

JP

(71) 出願人 (米国を除くすべての指定国について)

ローム株式会社(ROHM CO., LTD.)(JP/JP)

〒615-0045 京都府京都市右京区西院溝崎町21番地 Kyoto, (JP)

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ)

疋田純一(HIKITA, Junichi)(JP/JP)

生藤義弘(IKEFUJI, Yoshihiro)(JP/JP)

田口治生(TAGUCHI, Haruo)(JP/JP)

〒615-0045 京都府京都市右京区西院溝崎町21番地

ローム株式会社内 Kyoto, (JP)

(74) 代理人

弁理士 深見久郎, 外(FUKAMI, Hisao et al.)

〒530-0054 大阪府大阪市北区南森町2丁目1番29号

住友銀行南森町ビル Osaka, (JP)

(81) 指定国 AU, CA, CN, KR, US, 欧州特許 (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

添付公開書類

国際調査報告書

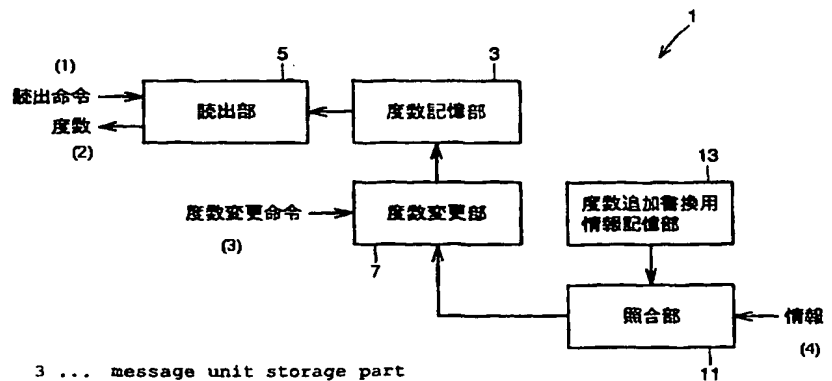
補正書

(54)Title: PORTABLE MESSAGE UNIT STORAGE MEMBER AND ITS USING METHOD

(54)発明の名称 可搬性を有する度数記憶部材およびその使用方法

(57) Abstract

A message unit storage part (3) has a plurality of data holding parts the number of which is equal to the value of the message unit. A message unit adding/rewriting information storage part (13) stores the message unit adding/rewriting information. A collation part (11) collates the given information with the message unit adding/rewriting information. A message unit changing part (7) can change the states of the respective data holding parts from 1st states to 2nd states only. However, the data changing part (7) may also change the states of the respective data holding parts from the 2nd states to the 1st states in accordance with the collation results of the collation part (11). That is, the states of the respective data holding parts can be normally changed from the 1st states to the 2nd states (change in the direction in which the message unit decreases) only. Thus, a message unit storage member which is difficult to alter can be provided.



3 ... message unit storage part

5 ... reading part

7 ... message unit changing part

11 ... collation part

(1) ... reading instruction

(2) ... message unit

(3) ... message unit changing instruction

(4) ... information

13 ... message unit adding/rewriting information storage part

(57) 要約

度数記憶部(3)は、データ保持部を度数の個数分有する。度数追加書換用情報記憶部(13)は、度数追加書換用情報を記憶する。照合部(11)は、与えられた情報と度数追加書換用情報とを照合する。度数変更部(7)は、各データ保持部を第1の状態から第2の状態にのみ変更可能である。ただし、度数変更部(7)は、照合部(11)の照合結果に基づいて、各データ保持部を第2の状態から第1の状態にも変更できる。すなわち、各データ保持部においては通常は第1の状態から第2の状態への変更(度数が減少する方向への変更)のみが可能である。これにより変造が困難な度数記憶部材を提供することができる。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AL	アルバニア	FI	フィンランド	LT	リトアニア	SN	セネガル
AM	アルメニア	FR	フランス	LU	ルクセンブルグ	SZ	スワジランド
AT	オーストリア	GB	イギリス	LV	ラトヴィア	TD	チャド
AU	オーストラリア	GE	グルジア	MC	モナコ	TG	トーゴ
AZ	アゼルバイジャン	GH	ガーナ	MD	モルドヴァ	TT	トリニダード・トバゴ
BA	ボスニア・ヘルツェゴビナ	GN	ギニア	MG	マダガスカル	TM	トルクメニスタン
BB	バルバドス	GW	ギニア・ビサウ	MK	マケドニア共和国	TR	トルコ
BE	ベルギー	GU	グアム	ML	マリ	TT	トリニダード・トバゴ
BG	ブルガリア	HU	ハンガリー	MN	モンゴル	UA	ウクライナ
BJ	ベナン	ID	インドネシア	MR	モーリタニア	UG	ウガンダ
BR	ブラジル	IE	アイルランド	MW	マラウイ	US	米国
BY	ベラルーシ	IL	イスラエル	NL	オランダ	UZ	ウズベキスタン
CA	カナダ	IS	アイスランド	NE	ニジェール	VN	ベトナム
CC	中央アフリカ共和国	IT	イタリア	NL	オランダ	YU	ユーゴスラヴィア
CF	コンゴ共和国	JP	日本	NO	ノルウェー	ZW	ジンバブエ
CG	コンゴ共和国	KE	ケニア	NZ	ニュージーランド		
CH	スイス	KG	キルギス	PL	ポーランド		
CI	コートジボワール	KR	韓国	PT	ポルトガル		
CM	カメルーン	KZ	カザフスタン	RO	ルーマニア		
CN	中国	LC	セント・ルシア	RU	ロシア		
CU	キューバ	LI	リヒテンシュタイン	SD	スーダン		
CC	キプロス	LK	スリランカ	SE	スウェーデン		
CZ	チェコ	LS	レソト	SG	シンガポール		
DE	ドイツ			SI	スロベニア		
DK	デンマーク			SK	スロバキア		
EE	エストニア			SL	シエラ・レオネ		
ES	スペイン						

明細書

可搬性を有する度数記憶部材およびその使用方法

5 技術分野

この発明は可搬性を有する度数記憶部材およびその使用方法に関するものであり、特に機密性を向上させた度数記憶部材およびその使用方法に関する。

背景技術

10 スキー場のリフトや鉄道の自動改札、荷物の自動仕分けなどに、ＩＣカードを用いたデータ通信システムが提案されている。

第１２図に、ＩＣカードを用いたデータ通信システムであって、非接触式ＩＣカードを用いた通信システムの構成を示す。このシステムは、質問器４０（たとえば、スキー場のリフトのゲート内に搭載される）と非接触ＩＣカード１００によって構成される。

質問器４０は、制御部４８の制御により、発振回路（OSC）４９からの高周波搬送波をアンテナ４１から送り出している。質問器４０に対して非接触ＩＣカード１００が接近すると、この高周波搬送波が非接触ＩＣカード１００のアンテナ２３によって受信される。電源生成回路２５は、受信した高周波を直流電力に変換して、他の回路部分に供給する。このようにして、質問器４０に近づくと、非接触ＩＣカード１００が動作可能となる。

また、質問器４０から非接触ＩＣカード１００に対する情報伝達は、前記高周波搬送波を変復調回路４６において変調することにより行なわれる。制御部３５は、復調された情報に基づき、メモリ３７の内容の変更や情報返信などの必要な処理を行なう。

一方、非接触ＩＣカード１００から質問器４０に対しての情報伝達も行なわれる。非接触ＩＣカード１００側には、発振回路が設けられていないので、次のようにして、情報送信が行なわれる。質問器４０の側から無変調の高周波搬送波を送り出しておき、非接触ＩＣカード１００側にて変復調回路３３により、共振回

路 2 2 のインピーダンスを変化させる。質問器 4 0 は、このインピーダンス変化を、自己側の共振回路 4 2 のインピーダンス変化として、変復調回路 4 6 により検出して復調する。制御部 4 8 は、復調された情報を得て、必要な処理を行なう。

5 非接触 I C カード 1 0 0 が質問器 4 0 から遠ざかると、電力供給がなくなるので、非接触 I C カード 1 0 0 の動作は停止する。なお、メモリ 3 7 は不揮発性メモリであるので、電力供給がなくなっても、記憶された情報は保持される。

以上のような非接触 I C カード 1 0 0 のメモリ 3 7 に所定の度数を記憶させておき、使用度数に応じてメモリ 3 7 のデータを変更することにより、プリペイドカードとして I C カードを用いることができる。

10 なお、質問器と I C カードとの間の通信データは暗号化される。これによって、一旦使用済の I C カードの内容が無断で変更されることが防止できる。

しかしながら、このような従来の I C カードを用いた通信システムは、次のような問題点があった。上記のように、通信データを暗号化しても、その暗号化アルゴリズムが解読されると、結局、データ変造が可能となる。したがって、暗号化のみではシステムの機密性を確保することが困難である。

特に、質問器を不特定多数の場所に配置するような場合、たとえば、公衆電話などにおいては、質問器が内蔵された電話機が盗まれることも考えられ、この場合質問器と I C カードとの間でやり取りされる命令が解析されるおそれもある。

20 この発明は、上記のような問題点を解決するためになされたものであり、不正使用が困難な、可搬性を有する度数記憶部材およびその使用方法を提供することをその目的としている。

発明の開示

25 上記目的を達成するため、この発明のある局面に従うと度数記憶部材は、金銭に対応する度数を記憶する可搬性を有する度数記憶部材であって、外部から与えられた読出命令に基づいて、記憶されている度数を読出し、外部から与えられた度数変更命令に基づいて、記憶されている度数を変更する変更手段を有し、度数が増加する方向への度数変更を回路構成的に禁止したことを特徴とする。

この発明に従うと、度数を増加させるデータ変更を確実に防止することができ

る。これにより、不正使用が困難な度数記憶部材を提供することができる。

好ましくは、可搬性を有する度数記憶部材は、予め度数追加書換用情報を記憶する度数追加書換用情報記憶手段をさらに備え、この度数追加書換用情報と一致する情報が与えられた場合には、回路構成を切換え、度数が増加する方向への度数変更を可能としたことを特徴とする。

この発明に従うと、必要な場合にのみ、増加方向への度数変更を防止することができる。

この発明の他の局面に従うと、可搬性を有する度数記憶部材は、金銭に対応する度数を記憶する記憶手段であって、書込データを保持可能なデータ保持部を度数の個数分有する度数記憶手段と、度数記憶部材の外部から与えられた読出命令に基づいて、度数記憶手段に記憶されている度数を読出す読出手段と、度数記憶部材の外部から与えられた度数変更命令に基づいて、度数記憶手段の各データ保持部を第1の状態から第2の状態にだけ変更可能な度数変更手段とを備えたことを特徴とする。

この発明に従うと、データ保持部を第1の状態から第2の状態にだけ変更することが可能なため、不正なデータ変更を確実に防止することができる。

さらに好ましくは、可搬性を有する度数記憶部材は、度数追加書換用情報を記憶する度数追加書換用情報記憶手段と、与えられた情報と度数追加書換用情報とを照合する照合手段とをさらに備え、度数変更手段は、各データ保持部を第1の状態から第2の状態に変更可能なだけでなく、さらに照合手段の照合結果に基づいて、各データ保持部を第2の状態から第1の状態にも変更可能であることを特徴とする。

この発明に従うと、予め記憶させた度数追加書換用情報と対応する情報が与えられた場合にだけ、各データ保持部を第2の状態から第1の状態へ変更することが可能となる。これにより、不正なデータ変更を確実に防止することができる。

この発明の他の局面に従うと、可搬性を有する度数記憶部材の使用方法是、可搬性を有する度数記憶部材に金銭に対応する度数を記憶しておき、外部から与えられた読出命令に基づいて度数記憶部材に記憶された度数を読出すとともに、外部から与えられた度数変更命令に基づき度数を変更する度数記憶部材の使用方法是、

であって、度数が増加する方向への度数変更を回路構成的に禁止したことを特徴とする。

さらに好ましくは、可搬性を有する度数記憶部材の使用方法は、度数記憶部材に予め度数追加書換用情報を記憶しておき、この度数追加書換用情報と一致する
5 情報が与えられた場合には、回路構成を切換え、度数が増加する方向への度数変更を可能としたことを特徴とする。

この発明のさらの他の局面に従うと、可搬性を有する度数記憶部材の使用方法は、度数記憶部材に金銭に対応する度数を記憶しておき、外部から与えられた読
10 出命令に基づいて度数記憶部材に記憶された度数を読出すとともに、外部から与えられた度数変更命令に基づき度数を変更する度数記憶部材の使用方法であって、
度数記憶部材は、度数に対応する個数分のデータ保持部を有しており、各データ保持部は、第1の状態から、第2の状態にだけ変更されることが可能であり、度
数記憶部材は、各データ保持部の状態に基づいて度数を記憶することを特徴とする。

さらに好ましくは、可搬性を有する度数記憶部材の使用方法は、度数記憶部材に予め度数追加書換用情報を記憶させておき、この度数追加書換用情報と一致す
15 る情報が与えられた場合には、各データ保持部を第1の状態から第2の状態に変更可能なだけでなく、さらに各データ保持部を第2の状態から第1の状態にも変更可能としたことを特徴とする。

この発明のさらに他の局面に従うと、度数記憶部材は度数を記憶する記憶手段と、記憶手段に記憶された度数を変更させる変更手段と、変更手段が度数を増加
20 させることを禁止する禁止手段とを備える。

さらに好ましくは度数記憶部材は、検証対象となるデータを入力する入力手段と、入力されたデータと所定の暗号とを比較する比較手段とをさらに備え、禁止
25 手段は、比較手段の比較結果に基づいて度数を増加させることを禁止する。

図面の簡単な説明

第1図は、本発明の実施の形態の1つにおける度数記憶部材1の機能ブロックを示す図である。

第2図は、本発明の実施の形態の1つにおけるICカード10の構成の概略を示す図である。

第3図は、第2図における制御部60およびメモリ部50の詳細を示す図である。

5 第4図は、メモリ部50の構造を示す模式図である。

第5図は、読出、書込、消去および動作禁止電圧の一例を示す図である。

第6図は、読出変更回路61、暗号照合部63、およびメモリエリア選択検知回路67の相関関係を説明するための図である。

第7図は、暗号照合部63の詳細を示す図である。

10 第8図は、ICカード10の動作を説明するためのフローチャートである。

第9図は、第8図に続くフローチャートである。

第10図は、第9図に続くフローチャートである。

第11図は、第8図に続くフローチャートである。

15 第12図は、従来のICカード100およびその質問器40の構成を示すブロック図である。

発明を実施するための最良の形態

本発明をより詳細に説明するために、添付の図面に従ってこれを説明する。

[1. ICカードの機能ブロックについて]

20 第1図を参照して、本発明の実施の形態の1つにおける度数記憶部材1について説明する。度数記憶部材1は、可搬性を有し、度数記憶部3と、読出部5と、度数変更部7と、度数追加書換用情報記憶部13と、照合部11とを備えている。

25 度数記憶部3は、金銭に対応する度数を記憶する記憶部であって、書込データを保持可能なデータ保持部を前記度数個数分有する。読出部5は、度数記憶部材の外部から与えられた読出命令に基づいて、度数記憶部3に記憶されている度数を読出す。度数変更部7は、度数記憶部材の外部から与えられた度数変更命令に基づいて、度数記憶部3の前記各データ保持部を書込データを保持しない非書込状態（第1の状態）から書込データを保持する書込状態（第2の状態）にだけ変更できる。

また、度数追加書換用情報記憶部 13 は、度数追加書換用情報を記憶する。照
合部 11 は、与えられた情報と前記度数追加書換用情報とを照合する。度数変更
部 7 は、各データ保持部を非書込状態から書込状態に変更できるだけでなく、
さらに、照合部 11 の照合結果に基づいて、各データ保持部を書込状態から非書
込状態にも変更できる。

ここで、非書込状態にあるデータ保持部の数を残り度数とすると、度数を増加
させるデータ変更を確実に防止できるとともに、予め記憶させた度数追加書換用
情報と一致する情報が得られた場合にだけ、度数を増加させる変更が可能である。

[2. ICカードの具体的な構成について]

次に、本発明を非接触 IC カードに適用した場合について第 2 図を用いて説明
する。

非接触 IC カード 10 は、全体構成としては、従来と同様に、アンテナ 23 と、
共振回路 22 と、電源生成回路 25 と、変復調回路 33 と、制御部 60 と、メモ
リ 50 とが筐体 11 に収納されている構成を取っている。なお、筐体 11 への収
納方法、電源の供給方法およびデータの送受信方法については、従来の技術と同
様であるので説明は繰返さない。

第 3 図は、第 2 図に示される制御部 60 およびメモリ部 50 の詳細を示すブロ
ック図である。メモリ部 50 は、度数エリア 51、設定情報エリア 52、機密デ
ータエリア 53 および機密データエリア 54 を有する。度数エリア 51 は、度数
を記憶するエリアであり、設定情報エリア 52 は設定情報を記憶するエリアであ
る。機密データエリア 53 は、IC カード運用者の暗号を記憶するエリアである。
機密データエリア 54 は、IC カード製造者の機密データを記憶するエリアであ
る。

度数エリア 51 は第 3 図に示すように、128 バイト (1024 ビット) のデ
ータを記憶可能である。設定情報エリア 52 は 32 バイト、機密データエリア 5
3 は 3 バイト、機密データエリア 54 は 3 バイトのデータが記憶可能である。

[2. 1 メモリ部 50]

メモリ部 50 のメモリ構造について、第 4 図および第 5 図を参照して説明する。
本実施の形態においては、不揮発性メモリとして EEPROM を採用した。メモ

リ部50は、第4図に示されるようなセルC11がマトリックス状に配置されることにより構成される（図示せず）。

セルC11のデータを変更する場合（データ書込：データ「0」を保持させること、データ消去：データ「1」を保持させること）、データを読み出す場合の、
5 ビットラインBL、選択ラインSL、ワードラインWLに印加する電圧を第5図に示す。

メモリセルC11を書込状態とする（データ「0」を保持させる）場合には、ビットラインBLに20（V）を、選択ラインSLに0（V）を、ワードラインWLに20（V）の電圧を印加し、ラインAGを開状態とする。これにより、セルC11のフローティングゲートに電子が注入され、データ「0」が保持される状態となる。
10

メモリセルC11を消去状態とする（データ「1」を保持させる）場合には、データ「0」を保持させるのと逆方向の電圧を印加すればよい。すなわち、ビットラインBLに0（V）を、選択ラインSLに20（V）を、ワードラインWLに20（V）の電圧を印加し、ラインAGを開状態（または0（V））とする。これにより、セルC11のフローティングゲートから電子が放出され、データ「1」が保持される状態となる。
15

メモリセルC11の情報を読み出す場合には、選択ラインSLに5（V）の電圧を印加し、ワードラインWLに5（V）の電圧を、かつビットラインBLにセンスアンプ（図示せず）を接続する。メモリセルC11が「0」または「1」のいずれを記憶しているかによって、センスアンプにおける検出結果が変わる。これにより、メモリセルC11にデータ「1」またはデータ「0」が保持されているかを知ることができる。
20

このように、度数エリア51の各メモリセルは、データ「0」またはデータ「1」を記憶しており、メモリセルの各々がデータ保持部を構成する。また、度数エリア51は予め設定された度数に対応する個数分メモリセルを有する。すなわち、度数が1000度数であれば1000ビット分のメモリセルを有する。
25

設定情報エリア52、機密データエリア53、機密データエリア54については従来と同様、通常のビット長でデータを保持するようにしている。

[2. 2 制御部 6 0]

次に、制御部 6 0 について第 3 図を用いて説明する。制御部 6 0 は、主制御部 6 9、アドレスデコーダ 6 5、メモリエリア選択検知回路 6 7、暗号照合部 6 3 および読出変更回路 6 1 を有する。

- 5 主制御部 6 9 は、変復調回路 3 3 から与えられたデータに基づきアドレスを指定し、アドレスデコーダ 6 5 にアドレスを与える。さらに、読出変更回路 6 1 に対し、読出、書込、消去のいずれかの命令を与える。また、暗号照合部 6 3 に対し、照合対象となる暗号を与える。アドレスデコーダ 6 5 によって選択されたアドレスは、メモリエリア選択検知回路 6 7 によって検知され、メモリエリア選択
10 検知回路 6 7 は、暗号照合部 6 3 および読出変更回路 6 1 に選択アドレスを与える。

[2. 2. 1 読出変更回路 6 1]

- 読出変更回路 6 1 は、主制御部 6 9 から与えられる命令に応じて、第 5 図に示す読出電圧、書込電圧、消去電圧、または後述する動作禁止電圧をメモリ部 5 0
15 に与える。

- 読出変更回路 6 1 について、第 6 図を用いて説明する。読出変更回路 6 1 は、選択アドレス特定端子 T s 1 ~ T s 3、モード端子 T e、モード端子 T f を有する。選択アドレス特定端子 T s 1 ~ T s 3 には、いずれのエリアが選択されているかを示す信号がメモリエリア選択検知回路 6 7 から与えられる。具体的には、
20 度数エリア 5 1 が選択されている場合には、選択アドレス特定端子 T s 1 には電圧「H i g h」が与えられる。設定情報エリア 5 2 が選択されている場合には、選択アドレス特定端子 T s 2 には電圧「H i g h」が与えられる。機密データエリア 5 3 が選択されている場合には、選択アドレス特定端子 T s 3 には電圧「H i g h」が与えられる。

- 25 また、モード端子 T e、モード端子 T f には、暗号照合部 6 3 から信号が与えられる。本実施の形態においては、読出変更回路 6 1 では、2 つのモード端子に印加される電圧に応じて、以下の 3 つのモードが切換えられる。

モード端子 T f に電圧「L o w」が、モード端子 T e に電圧「L o w」が与えられた状態が、モード「0, 0」（通常モード）である。

また、モード端子T_fに電圧「L o w」が、モード端子T_eに電圧「H i g h」が与えられた状態がモード「0, 1」（度数書換モード）である。

また、モード端子T_fに電圧「H i g h」が、モード端子T_eに電圧「L o w」が与えられた状態がモード「1, 0」（初期化モード）である。

- 5 読出変更回路61は、後述するように、選択アドレス特定端子T_{s1}～T_{s3}、モード端子T_e、モード端子T_fに与えられている電圧に応じて、動作禁止電圧をメモリ50の各エリアに印加する。

- 10 各モードにおいて、読出変更回路61が印加可能な電圧について説明する。モード「0, 0」においては、選択アドレス特定端子T_{s1}～T_{s3}によって特定される選択アドレスが度数エリア51または設定情報エリア52である場合には、第5図に示す書込電圧を出力可能である。しかし、消去電圧については出力できない。

- 15 モード「1, 0」においては、選択アドレス特定端子T_{s1}～T_{s3}によって特定される選択アドレスが度数エリア51または設定情報エリア52である場合には、第5図に示される書込電圧および消去電圧を出力できる。しかし、選択アドレス特定端子T_{s1}～T_{s3}によって特定される選択アドレスが、機密データエリア53、54である場合には、第5図に示す書込電圧または消去電圧を出力できない。すなわち、第5図に示す書込および消去については、度数エリア51、設定情報エリア52のみで可能となる。

- 20 モード「1, 0」においては、選択アドレス特定端子T_{s1}～T_{s3}によって特定される選択アドレスが、度数エリア51、設定情報エリア52または機密データエリア53である場合には、第5図に示す消去電圧を出力できる。しかし、選択アドレスが機密データエリア54である場合には、消去電圧を出力できない。また、書込電圧については、いずれのエリアに対しても出力できない。

- 25 なお、機密データエリア53、機密データエリア54のデータ線は、第3図に示すように暗号照合部63に接続されている。したがって、読出された暗号が主制御部69に与えられることがなく、外部から機密データエリア53および機密データエリア54に記憶された暗号が読出されることを防止できる。

[2. 2. 2 暗号照合部63]

暗号照合部 6 3 は、メモリエリア選択検知回路 6 7 から検知信号が与えられると動作可能状態となり、機密データエリア 5 3 または機密データエリア 5 4 に記憶された暗号と主制御部 6 9 から与えられた信号が一致するか否かを判断する。両者が一致する場合には、読出変更回路 6 1 のモード端子 T e, T f へ電圧「H i g h」を与える。

第 7 図を用いて暗号照合部 6 3 の詳細について説明する。暗号照合部 6 3 は、比較器 7 1、比較器 7 3、およびデータ変換回路 7 5 を有する。比較器 7 3 は、機密データエリア 5 4 に記憶された I C カード製造者用暗号と一致する暗号が主制御部 6 9 から与えられた場合に、モード端子 T f へ電圧「H i g h」を与える。

また、比較器 7 1 はデータ変換回路 7 5 から与えられたデータおよび機密データエリア 5 3 より与えられたデータを合体させた暗号と一致する暗号が主制御部 6 9 から与えられた場合に、モード端子 T e へ電圧「H i g h」を与える。

たとえば、機密データエリア 5 4 に暗号「1 0 1 0 0 0 0 0」が記憶されており、I C カード運用者が自己の暗号として「1 0 1 0」を機密データエリア 5 3 に記憶させた場合、次のようにして照合が行なわれる。機密データエリア 5 4 の暗号「1 0 1 0 0 0 0 0」をデータ変換回路 7 5 が変換する。変換結果が「0 1 0 1 1 1 1 1」である場合は、比較器 7 1 には、機密データエリア 5 3 に記憶された I C カード運用者の暗号「1 0 1 0」の後に、「0 1 0 1 1 1 1 1」が付加された暗号「1 0 1 0 0 1 0 1 1 1 1 1」が与えられる。そして、比較器 7 1 は主制御部 6 9 から与えられた照合対象の入力データが、前記暗号「1 0 1 0 0 1 0 1 1 1 1 1」と一致するか否かを判断する。

なお、比較器 7 1 が、主制御部 6 9 から与えられたデータから、データ変換回路 7 5 からのデータを取除いて、機密データエリア 5 3 に記憶された暗号と比較するようにしてもよい。

また、本実施の形態においては、I C カード運用者は、I C カード製造者から、機密データエリア 5 4 の暗号をデータ変換回路 7 5 が変換したデータを得て、これを自己の暗号に付加して、照合すべき暗号として主制御部 6 9 に与えるようにする必要がある。

このように、本実施の形態においては、機密データエリア 5 4 の暗号をデータ

変換して、機密データエリア 5 3 の暗号に付加して、主制御部 6 9 から与えられた照合対象暗号データと比較するようにしている。したがって、I C カード製造者が I C カード運用者ごとに異なる暗号を機密データエリア 5 3 に記憶させることにより、たまたま 2 つの I C カード運用者が同じ暗号を機密データエリア 5 3 に記憶させた場合でも、混同が生じることはない。つまり一方の運用者が間違

5 3 に記憶させた場合でも、混同が生じることはない。つまり一方の運用者が間違

って他方の I C カード運用者の I C カードのデータを消去することはできないこととなる。

なお、いずれの比較器にて照合するかは、メモリエリア選択検知回路 6 7 から与えられる信号によって決定される。すなわち、検知したエリアが機密データエリア 5 4 である場合には比較器 7 3 に、機密データエリア 5 3 である場合には比較器 7 1 および比較器 7 3 に、照合処理を可能とする信号が与えられる。

10 リア 5 4 である場合には比較器 7 3 に、機密データエリア 5 3 である場合には比較器 7 1 および比較器 7 3 に、照合処理を可能とする信号が与えられる。

[3. I C カードの処理について]

次に、第 8 図～第 1 1 図を用いてデータの読出、書込、消去、暗号照合の処理について説明する。なお、初期状態（図示しないステップ S T 1）では、読出変更回路 6 1 のモード端子 T e、T f にはそれぞれ電圧「L o w」が与えられており、モード「0, 0」とされている。

15 更回路 6 1 のモード端子 T e、T f にはそれぞれ電圧「L o w」が与えられており、モード「0, 0」とされている。

次に、主制御部 6 9 は、変復調回路 3 3 から与えられた命令が読出命令か、残度数削除命令か、データ変更命令か、初期化命令かを判断する（ステップ S T 3）。

[3. 1 読出処理]

与えられた命令が読出命令である場合には、度数エリア 5 1 の全部のアドレスを選択する（ステップ S T 5）。そして、読出信号を出力する（ステップ S T 7）。これにより、度数エリア 5 1 の全データが読出され、主制御部 6 9 に与えられる（ステップ S T 8）。主制御部 6 9 は与えられたデータのうち、データ「1」が保持されているビットの個数（残度数）をカウントし、一時記憶する（ステップ S T 9）。次に、設定情報エリア 5 2 の全部のアドレスを選択する（ステップ S T 1 1）。そして、読出変更回路 6 1 へ読出信号を出力する（ステップ S T 1 3）。これにより、設定情報エリア 5 2 に記憶された設定情報が主制御部 6 9 に与えられる（ステップ S T 1 4）。主制御部 6 9 はこれを一時記憶す

25 「1」が保持されているビットの個数（残度数）をカウントし、一時記憶する（ステップ S T 9）。次に、設定情報エリア 5 2 の全部のアドレスを選択する（ステップ S T 1 1）。そして、読出変更回路 6 1 へ読出信号を出力する（ステップ S T 1 3）。これにより、設定情報エリア 5 2 に記憶された設定情報が主制御部 6 9 に与えられる（ステップ S T 1 4）。主制御部 6 9 はこれを一時記憶す

る（ステップS T 1 5）。主制御部 6 9は、変復調回路 3 3 へ一時記憶したデータ
を出力する（ステップS T 1 7）。

これにより外部に度数エリア 5 1に記憶された残度数および設定情報エリア 5
2に記憶された設定情報を出力することができる。

5 [3 . 2 度数削除処理]

次に、ステップS T 3において残度数削除命令が与えられた場合について説明
する。この場合、主制御部 6 9は、ステップS T 9で一時記憶した残度数を讀出
す（ステップS T 1 9）。そして、データ「1」が保持されている度数エリア 5
1のメモリセルの先頭のアドレスを選択する（ステップS T 2 1）。主制御部 6
10 9は、讀出変更回路 6 1へ書込信号（データ「0」を保持させる信号）を与える
（ステップS T 2 3）。

讀出変更回路 6 1は、この書込信号を受けて、第 6 図に示す選択アドレス特定
端子およびモード端子に与えられている電圧に応じて、書込電圧を印加できる状
態であるかどうかを判断する。この場合、選択アドレスは度数エリア 5 1であり、
15 モード端子はステップS T 1においてモード「0, 0」となっているので、書込
可能であると判断し、第 5 図に示す書込電圧を出力する（ステップS T 2 4）。

次に、主制御部 6 9はステップS T 9において一時記憶した残度数をデクリメ
ントする（ステップS T 2 5）。そして、残度数削除処理が終了したメッセージ
を変復調回路 3 3へ出力する（ステップS T 2 7）。これにより、残度数を削除
20 する命令が与えられた場合に、度数エリア 5 1に記憶された度を指定された分
だけ減方向に変更することができる。このようにして、予め度数エリア 5 1に記
憶された度を讀出し、または度数削除命令に応じて度を減らす方向にデータ
を変更することができる。

 [3 . 3 データ変更処理]

25 次に、ステップS T 3にて、データ変更命令が与えられた場合について説明す
る。データ変更命令は、度数エリア 5 1または設定情報エリア 5 2のデータを変
更する命令であり、機密データエリアに記憶された暗号を照合する照合命令を含
む。

この場合、主制御部 6 9は機密データエリア 5 3、5 4のアドレスを選択する

(第9図のステップST51)。次に、暗号照合部63へ検証対象データを出力する(ステップST53)。主制御部69は読出変更回路61へ読出信号を出力する(ステップST55)。これにより、読出変更回路61は読出電圧を印加する(ステップST56)。暗号照合部63は、機密データエリア53、54から読出された暗号と、主制御部69から与えられた検証対象データとの照合を行なう(ステップST57)。

具体的には既に説明したように、機密データエリア54に記憶された暗号がデータ変換回路75(第7図参照)に与えられる。データ変換回路75は所定の規則に基づいてこの暗号を変換し、変換結果を比較器71に与える。また、比較器71には機密データエリア53に記憶されている暗号が与えられる。比較器71はデータ変換回路75から与えられたデータおよび機密データエリア53より与えられたデータを合体させ、入力された検証対象データと一致するか否かを判断する。一致した場合には、比較器71は読出変更回路61に対しモード端子Teに電圧「High」を与える。これにより、読出変更回路61は、モード「0, 1」となる(第10図ステップST61)。

次に、主制御部69は、度数エリア51および設定情報エリア52の全アドレスを選択する(ステップST63)。次に、読出変更回路61に消去信号を出力する(ステップST65)。ここで、読出変更回路61については、モード「0, 1」であり、かつ選択アドレスが度数エリア51および設定情報エリア52であるので、消去電圧を出力可能である。したがって、読出変更回路61は消去電圧を印加する(ステップST66)。かかる消去電圧が与えられると、度数エリア51および設定情報エリア52のすべてのビットに「1」が保持される。

次に、主制御部69は、度数エリア51、設定情報エリア52のうち、必要なビットのみ選択する(ステップST67)。たとえば、設定情報エリア52に消去日時などを再度書込む必要がある。このような場合に、データ「0」を保持するビットを選択する。

主制御部69は、読出変更回路61へ書込信号を出力する(ステップST69)。読出変更回路61は書込電圧を印加する(ステップST70)。これにより、選択されたビットのみデータ「0」が保持される。そして、主制御部69は、

終了メッセージを変復調回路 3 3 へ与える（ステップ S T 7 1）。

なお、第 9 図のステップ S T 5 9 にて与えられた検証対象データが不一致である場合には、主制御部 6 9 は、度数エリア 5 1 および設定情報エリア 5 2 の全アドレスを選択する（第 1 0 図ステップ S T 7 3）。次に、読出変更回路 6 1 に消去信号を出力する（ステップ S T 7 5）。読出変更回路 6 1 は、現在のモードが、モード「0, 0」であるので、消去電圧を出力せずに動作禁止電圧を出力する（ステップ S T 7 7）。したがって、度数エリア 5 1 および設定情報エリア 5 2 の内容は変化しない。

なお、本実施の形態においては、動作禁止電圧として、ライン A G を接地電位とするとともに、他のラインについては開状態とした。

次に、主制御部 6 9 は、度数エリア 5 1、設定情報エリア 5 2 のうち、必要なビットのみ選択する（ステップ S T 7 9）。主制御部 6 9 は、読出変更回路 6 1 へ書込信号を出力する（ステップ S T 8 1）。ここで、現在のモードが「0, 0」で、選択アドレスが度数エリア 5 1 および設定情報エリア 5 2 であるので、読出変更回路 6 1 は書込電圧を出力せずに動作禁止電圧を出力する（ステップ S T 8 3）。したがって、度数エリア 5 1 および設定情報エリア 5 2 の内容は変化しない。そして、主制御部 6 9 は再書込ができなかった旨をメッセージ出力する（ステップ S T 8 5）。

このように、暗号不一致の場合には、主制御部 6 9 から、読出変更回路 6 1 に対して消去信号および書込信号を出力しても、読出変更回路 6 1 は書込電圧および消去電圧を印加しない。

このようにして、予め I C カード運用者が入力した暗号と、I C カード製造者から与えられたデータとに対して、一致する暗号が与えられた場合にだけ、度数エリア 5 1 および設定情報エリア 5 2 のデータを変更することができる。したがって、機密性の高い I C カードを提供することができる。

[3. 4 初期化处理]

次に、第 8 図のステップ S T 3 において、初期化命令が与えられた場合について、第 1 1 図を用いて説明する。初期化命令とは、機密データエリア 5 4 以外の度数エリア 5 1、設定情報エリア 5 2、および機密データエリア 5 3 のデータを

すべて「1」とする命令を言い、ICカード製造者が行なうものである。

この場合、主制御部69は、機密データエリア54のアドレスを選択するとともに（ステップST31）、暗号照合部63へ検証対象データを出力する（ステップST32）。主制御部69は、読出変更回路61へ読出信号を出力する（ステップST33）。読出変更回路61は、読出電圧を印加する（ステップST34）。暗号照合部63において暗号が照合される（ステップST35）。この場合は機密データエリア54に記憶されたデータが比較器73に与えられ、比較器73は主制御部69より与えられた検証対象データと機密データエリア54に記憶された暗号が一致するか否かを判断する（ステップST36）。

第11図のステップST36において、照合結果が一致すると判断した場合には、暗号照合部63は、読出変更回路61のモード端子Tfに電圧「High」を与える（ステップST37）。これにより、読出変更回路61はモード「1，0」となる。

次に、主制御部69は、度数エリア51、設定情報エリア52、および機密データエリア53の全アドレスを選択する（ステップST38）。そして、読出変更回路61へ消去信号を出力する（ステップST39）。ここで、読出変更回路61のモードは、モード「1，0」であるので、読出変更回路61は消去電圧を印加する（ステップST41）。これにより、度数エリア51、設定情報エリア52、および機密データエリア53の全データが初期化される。主制御部69は終了メッセージを変復調回路33へ出力する（ステップST42）。

なお、第11図のステップST36において、照合不一致の場合には、読出変更回路61のモード端子Tfへ電圧「High」が与えられない。したがって読出変更回路61はモード「0，0」のままである。主制御部69は、度数エリア51、設定情報エリア52、および機密データエリア53の全アドレスを選択する（ステップST43）。そして、読出変更回路61へ消去信号を出力する（ステップST44）。ここで、読出変更回路61のモードは、モード「0，0」であり、選択アドレスが度数エリア51、設定情報エリア52、および機密データエリア53であるので、読出変更回路61は動作禁止電圧を印加する（ステップST45）。すなわち、度数エリア51、設定情報エリア52、および機密デー

タエリア 5 3 の全データは初期化されない。主制御部 6 9 は初期化不能メッセージを変復調回路 3 3 へ出力する（ステップ S T 4 6）。

このように、初期化命令が与えられた場合でも、機密データエリア 5 4 に記憶された暗号と一致する検証対象データが与えられた場合にだけ、初期化を行なうことができる。

[3. 5 暗号記憶処理]

本実施の形態においては、機密データエリア 5 3 に I C カード運用者が暗号を記憶するために、機密データエリア 5 3 のデータが初期化された後、1 回に限り機密データエリア 5 3 のデータを変更可能としている。すなわち、初期化後、主制御部 6 9 に対して機密データエリア 5 3 のデータを変更するデータ変更命令が与えられた場合には、主制御部 6 9 は 1 回に限りデータ変更を認め、機密データエリア 5 3 に所定の暗号を記憶することができる。具体的には、これは第 1 0 図のステップ S T 6 1 からステップ S T 7 0 の処理を行なうことによって可能となる。

なお、主制御部 6 9 は、機密データエリア 5 3 のデータが変更されたかどうかを記憶しており、機密データエリア 5 3 のデータを変更する命令が再度与えられた場合には、これを無視する。

[4. 他の実施の形態]

なお、本実施の形態においては本発明を非接触の I C カードに適用した場合について説明したが、接触式の I C カードについても本発明を同様に適用することができる。

なお、主制御部 6 9 については C P U を用いて構成するようにしてもよく、また一部または全部をロジック回路で構成してもよい。読出変更回路 6 1、暗号照合部 6 3、およびメモリエリア選択検知回路 6 7 などについても同様である。

以上のように本実施の形態においては、度数エリア 5 1 にメモリセルを度数に対応する個数分設定しておく。モード「0, 0」である場合には、度数エリア 5 1 のメモリセルにデータ「1」が保持された非書込状態から、書込データ「1」が保持されていない書込状態にだけデータ変更を可能としている。これにより、I C カードの偽造をより確実に防止することができる。

また、通常の読出装置においては、度数エリア 5 1 のデータを減らす方向にのみ変更する命令しか I C カード側に提供しないので、いわゆる“なりすまし”による被害も防止することができる。

5 なお、メモリ 5 0 の構成については上記構成に限定されることなく、たとえば度数エリア 5 1 および設定情報エリア 5 2 を 1 つのメモリとし、機密データエリア 5 3、機密データエリア 5 4 を別のメモリで構成するようにしてもよい。

また、機密データエリア 5 3、機密データエリア 5 4 と 2 段階の暗号を設ける必要はなく、いずれか一方であってもよい。

10 なお、本実施の形態においては E E P R O M をメモリ部 5 0 に用いた場合について説明したが、データを変更できるものであれば、どのようなものでもよく、たとえば、フラッシュメモリ、強誘電体メモリなどであってもよい。

また、電氣的にデータを書込むだけでなく、光学的などの手段でデータを書き込めるものであっても、書込および消去の切換を行なえるものであれば同様に本発明を適用することができる。

15 なお、本実施の形態においては、暗号照合部からの照合結果が不一致である場合には、暗号照合部 6 3 から読出変更回路 6 1 の入力端子であるモード端子 T e および T f は、各々「L o w」のままである。したがって、読出変更回路 6 1 は、メモリ部 5 0 に対して動作禁止電圧を与えるだけであるので、データが変造されるおそれがない。

20 さらに、度数エリア 5 1 のデータを消去しようという信号が与えられた場合には、度数エリア 5 1 および設定情報エリア 5 2 の全ビットにデータ「0」を保持させるようにし、機密データエリア 5 4 の暗号が入れられない限り、再使用ができないようにしてもよい。

25 なお、本実施の形態においては暗号照合部 6 3 からの一致信号が与えられた場合にだけ、読出変更回路 6 1 のモード端子 T e、T f に電圧「H i g h」を与えるようにし、読出変更回路 6 1 にて主制御部 6 9 からのデータ変更信号を無視するようにしたが、主制御部 6 9 に対し照合不一致信号を与え、これに基づき、主制御部 6 9 がデータ変更ができないと判断し、読出変更回路 6 1 にデータ変更信号を出力しないようにしてもよい。そして、その旨のメッセージを表示するよう

にしてもよい。

また、本実施の形態においては、動作禁止電圧として、ラインAGを接地電位とするとともに、他のラインについては開状態としたが、要するに、書込または消去がされないような電圧であればどのようなものであってもよく、たとえば、

5 書込を禁止するにはビットラインBLに0（V）を印加してもよく、消去を禁止するには選択ラインSLに0（V）を印加するようにしてもよい。

なお、本実施の形態においては、データ「0」が書込まれている状態を書込状態、データ「1」が書込まれている状態を非書込状態、すなわちデータ「0」を書込データとしたが、データ「1」が書込まれている状態を書込状態、すなわち

10 データ「1」を書込データとしてもよい。

また、本実施の形態においては、フローティングゲートに電子が注入された状態をデータ「0」が保持された状態としたが、フローティングゲートから電子が引抜かれた状態をデータ「0」が保持された状態としてもよい。

なお、本実施の形態においては、初期状態でデータ「1」を保持したとき、度数を減らす場合には、対応するビットにデータ「0」を保持させるようにしたが、

15 逆に初期状態ではデータ「0」を保持させておき、度数を減らす場合には、対応するビットにデータ「1」を保持させるようにしてもよい。

また、本実施の形態においては、通常はモード端子Te、Tfへ電圧「Low」を与えて、度数エリア51の度数を減らす方向にのみ書換可能とするとともに、モード端子Te、Tfへ電圧「High」が与えられると、書込データを消去することを可能としているが、逆に通常はモード端子Te、Tfへ電圧「High」を与えておき、モード端子Te、Tfへ電圧「Low」が与えられると、書込データを消去可能となるようにしてもよい。

20

なお、本実施の形態においては、動作禁止電圧として、ラインAGを接地電位とするとともに、他のラインについては開状態とした。しかし、前記ラインAGを接地電位とするようにしてもよい。

25

なお上記実施の形態において度数エリア51はたとえば度数記憶部を構成する。主制御部69、アドレスデコーダ65、および読出変更回路61はたとえば読出部を構成する。主制御部69、アドレスデコーダ65、および読出変更回路61

たとえば度数変更部を構成する。機密データエリア 5 3 は度数追加書換用情報記憶部を構成する。また、たとえば暗号照合部 6 3 は照合部を構成する。

さらに、上記実施の形態において回路構成的に禁止するという表現は、特定の回路構成を採用することによりある処理をできなくすることを示す。すなわち、
5 論理回路または電気回路を用いて物理的にある処理を禁止することを言う。

なお、本実施の形態においては非書込状態（“1”）にあるデータ保持部の数を残り度数としたが、書込状態（“0”）にあるデータ保持部の数を残り度数としてもよい。すなわち、オールリセット状態ではデータ保持部をすべて“0”とし、度数の減少に伴い“1”としていてもよい。

10

産業上の利用可能性

以上のようにこの発明によれば不正使用が困難な度数記憶部材を提供することができるため、この発明は I C カードを製造、販売する分野に有利に適用することができる。

前記度数が増加する方向への度数変更を回路構成的に禁止したことを特徴とする、可搬性を有する度数記憶部材の使用方法。

6. 前記度数記憶部材に予め度数追加書換用情報を記憶しておき、

5 この度数追加書換用情報と一致する情報が与えられた場合には、前記回路構成を切換え、前記度数が増加する方向への度数変更を可能としたことを特徴とする、請求の範囲第5項記載の可搬性を有する度数記憶部材の使用方法。

7. 可搬性を有する度数記憶部材に金銭に対応する度数を記憶しておき、外部から与えられた読出命令に基づいて前記度数記憶部材に記憶された度数を読出すとともに、外部から与えられた度数変更命令に基づき前記度数を変更する度数記憶部材の使用方法であって、

前記度数記憶部材は、前記度数に対応する個数分のデータ保持部を有しており、前記各データ保持部は、第1の状態から、第2の状態にだけ変更されることが可能であり、

15 前記度数記憶部材は、前記各データ保持部の状態に基づいて度数を記憶することを特徴とする、可搬性を有する度数記憶部材の使用方法。

8. 前記度数記憶部材に予め度数追加書換用情報を記憶させておき、

20 この度数追加書換用情報と一致する情報が与えられた場合には、前記各データ保持部を前記第1の状態から前記第2の状態に変更可能なだけでなく、さらに前記各データ保持部を前記第2の状態から前記第1の状態にも変更可能としたことを特徴とする、請求の範囲第7項記載の可搬性を有する度数記憶部材の使用方法。

9. 度数を記憶する記憶手段と、

前記記憶手段に記憶された度数を変更させる変更手段と、

前記変更手段が前記度数を増加させることを禁止する禁止手段とを備えた、度数記憶部材。

25 10. 検証対象となるデータを入力する入力手段と、

前記入力されたデータと所定の暗号とを比較する比較手段とをさらに備え、

前記禁止手段は、前記比較手段の比較結果に基づいて前記度数を増加させることを禁止する、請求の範囲第9項記載の度数記憶部材。

補正書の請求の範囲

[1998年7月7日(07.07.98)国際事務局受理:出願当初の請求の範囲2, 4, 6及び10は取り下げられた;出願当初の請求の範囲1, 3, 5及び7-9は補正された;他の請求の範囲は変更なし。(3頁)]

請求の範囲

1. (補正後) 金銭に対応する度数を記憶する可搬性を有する度数記憶部材であって、

前記度数記憶部材の製造に係わる第1の業者が設定する第1暗号を記憶する第1暗号記憶部と、

前記度数記憶部材の運用に係わる前記第1の業者と異なる第2の業者が設定する第2暗号を記憶する第2暗号記憶部と、

外部から与えられた読出命令に基づいて、前記記憶されている度数を読出し、外部から与えられた度数変更命令に基づいて、前記記憶されている度数を減算する方向に変更する変更手段と、

前記第1暗号と第2暗号とに基づいて、前記変更手段による度数の変更を増加方向へも可能にすることの可否を判定する判定手段とを含む、可搬性を有する度数記憶部材。

2. (削除)

3. (補正後) 可搬性を有する度数記憶部材であって、

金銭に対応する度数を記憶する記憶手段であって、書込データを保持可能なデータ保持部を前記度数の個数分有する度数記憶手段と、

前記度数記憶部材の外部から与えられた読出命令に基づいて、前記度数記憶手段に記憶されている度数を読出す読出手段と、

前記度数記憶部材の製造に係わる第1の業者が設定する第1暗号を記憶する第1暗号記憶部と、

前記度数記憶部材の運用に係わる前記第1の業者と異なる第2の業者が設定する第2暗号を記憶する第2暗号記憶部と、

前記度数記憶部材の外部から与えられた度数変更命令に基づいて、前記度数記憶手段の前記各データ保持部を第1の状態と第2の状態との間で変更可能な度数変更手段と、

前記第1暗号と第2暗号とに基づいて、前記変更手段による度数の変更の可否を判定する判定手段とを含む、可搬性を有する度数記憶部材を備えたことを特徴とする、可搬性を有する度数記憶部材。

4. (削除)

5. (補正後) 可搬性を有する度数記憶部材に金銭に対応する度数と、前記度数

記憶部材の製造に係わる第1の業者が設定する第1暗号と、前記度数記憶部材の運用に係わる前記第1の業者と異なる第2の業者が設定する第2暗号とを記憶しておき、外部から与えられた読出命令に基づいて前記度数記憶部材に記憶された度数を読出すとともに、外部から与えられた度数変更命令に基づき前記度数を変更する度数記憶部材の使用方法であって、

前記度数変更命令に基づいて前記度数を増加する方向に変更する時は、前記第1暗号と第2暗号とに基づいて前記度数変更命令に従うか否かを判別することを特徴とする、可搬性を有する度数記憶部材の使用方法。

6. (削除)

7. (補正後) 可搬性を有する度数記憶部材に金銭に対応する度数を記憶しておき、外部から与えられた読出命令に基づいて前記度数記憶部材に記憶された度数を読出すとともに、外部から与えられた度数変更命令に基づき前記度数を変更する度数記憶部材の使用方法であって、

前記度数記憶部材は、前記度数に対応する個数分のデータ保持部を有し、

該各データ保持部の状態に基づいて度数を記憶し、第1から第2の状態にのみ変更するよう使用されるとともに、

前記度数記憶部材は、予め度数追加書換用情報を記憶し、

該度数追加書換用情報は、前記度数記憶部材の製造に係わる第1の業者が設定する第1暗号と、前記度数記憶部材の運用に係わる前記第1の業者と異なる第2の業者が設定する第2暗号とを含み、

この度数追加書換用情報と一致する情報が与えられた場合のみに、前記各データ保持部を第2の状態から第1の状態に変更するようにして使用することを特徴とする、度数記憶部材の使用方法。

8. (補正後) 前記度数追加書換用情報は前記第1暗号に対するデータと前記第2暗号に対するデータが異なるダイミングで入力されることを特徴とする、請求の範囲第7項に記載の度数記憶部材の使用方法。

9. (補正後) 度数を記憶する記憶手段と、

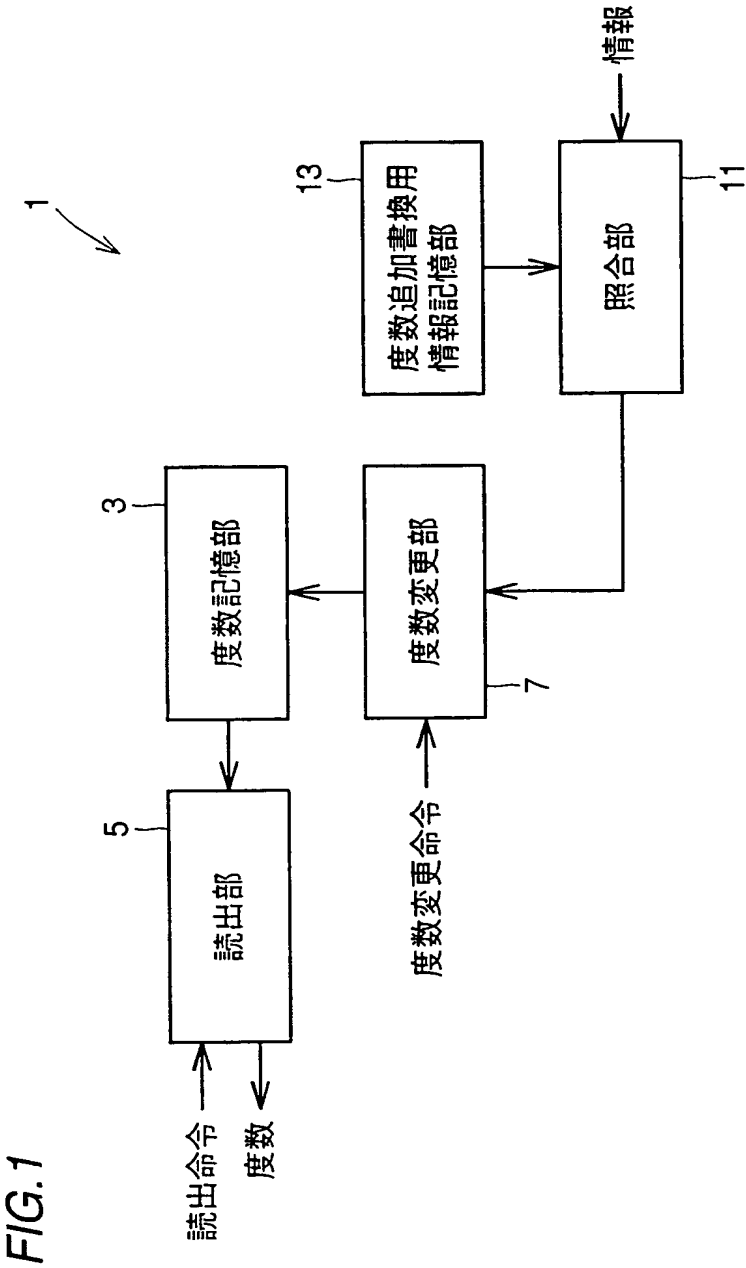
前記度数記憶部材の製造に係わる第1の業者が設定する第1暗号を記憶する第1暗号記憶部と、

前記度数記憶部材の運用に係わる前記第1の業者と異なる第2の業者が設定する第2暗号を記憶する第2暗号記憶部と

前記記憶手段に記憶された度数を変更させる変更手段と、
検証対象となるデータを入力する入力手段と、
前記入力手段から入力されたデータと前記第 1 および第 2 の暗号とを比較する
比較手段とを備え、

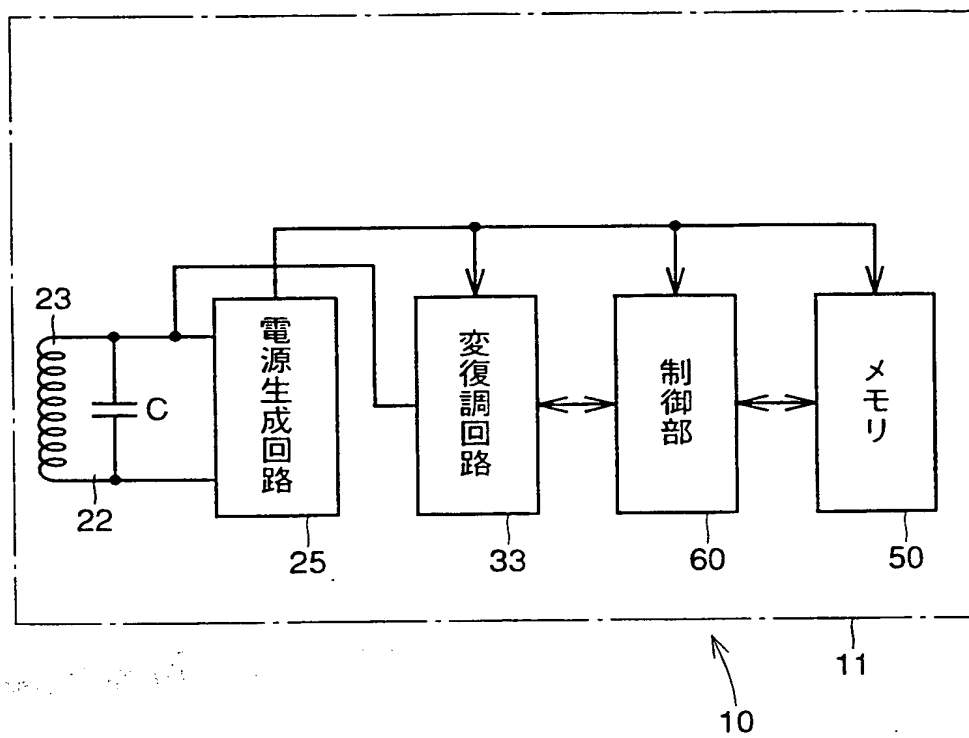
- 5 前記比較手段の比較結果に基づいて前記変更手段により、前記度数を増加させるか否かを判断する、度数記憶部材。

10. (削除)



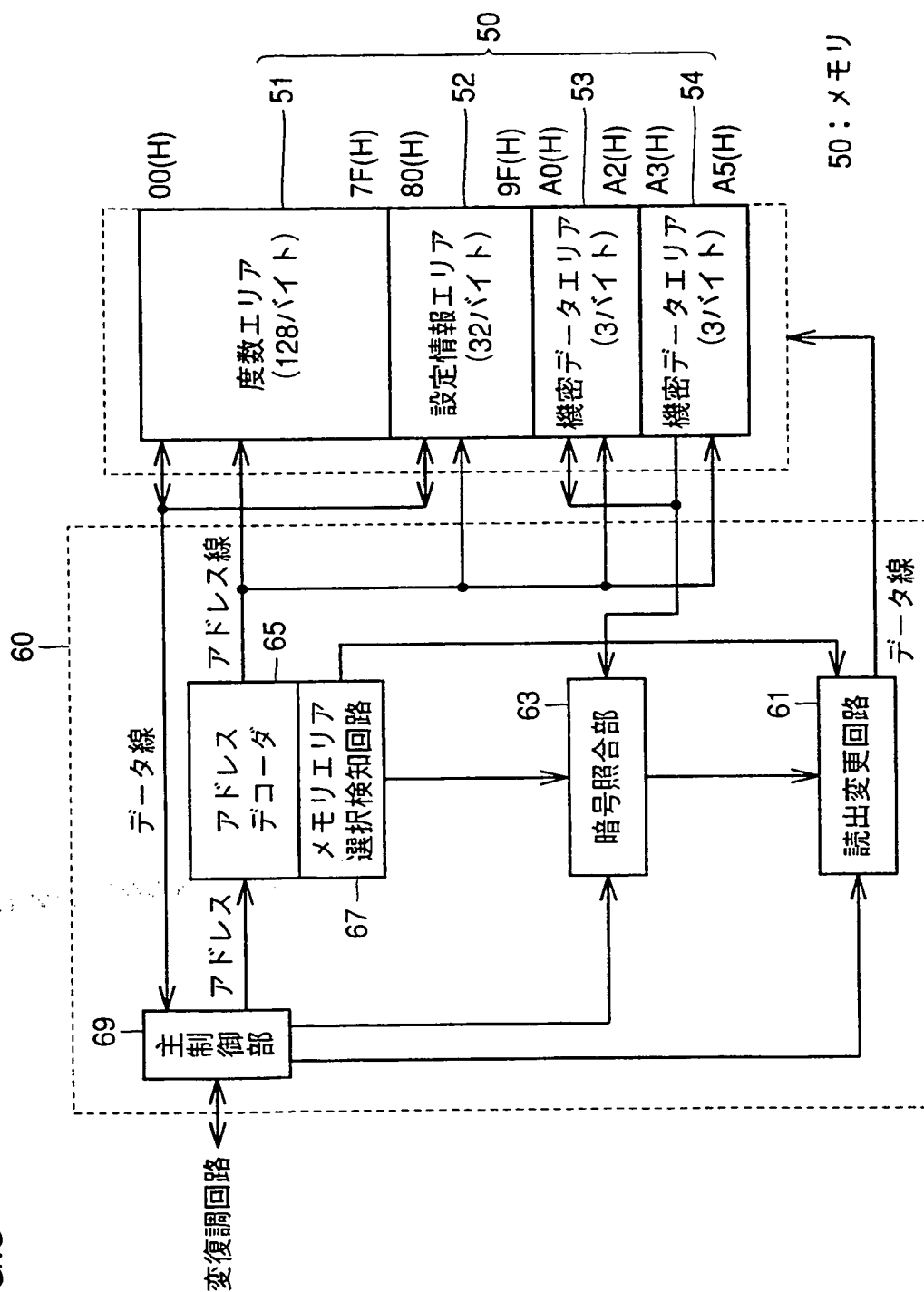
THIS PAGE BLANK (USPTO)

FIG.2



THIS PAGE BLANK (USPTO)

FIG.3



THIS PAGE BLANK (USPTO)

FIG.4

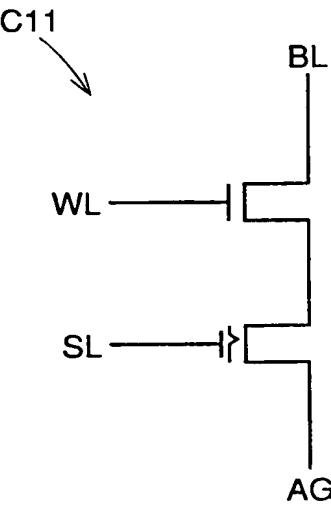


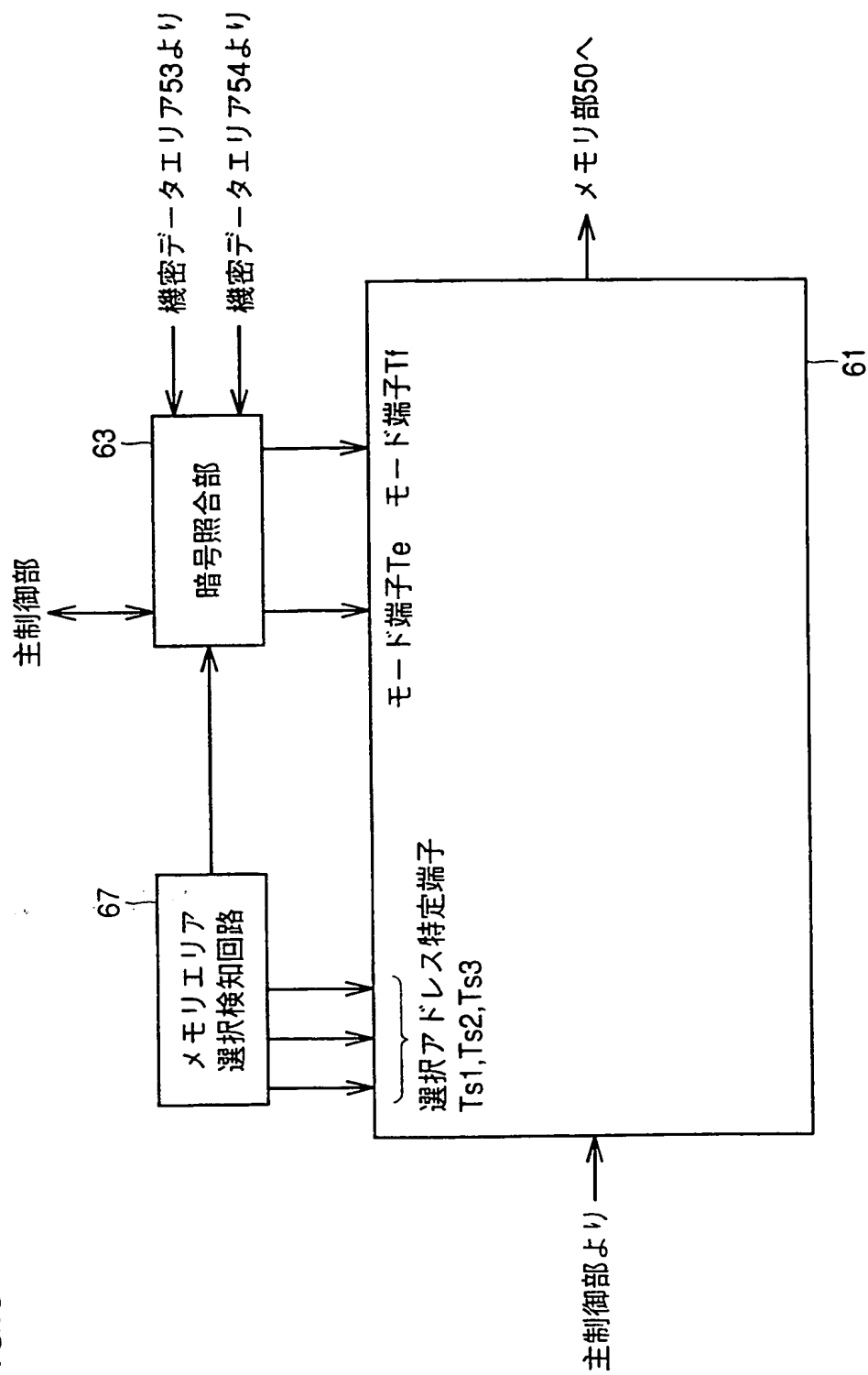
FIG.5

	BL	SL	WL	AG
読出	データ出力	5V	5V	0V
書込	20V	0V	20V	open
消去	0V	20V	20V	open or 0V

データ変更 { 書込 : 「1」 → 「0」 に書き換える
消去 : 「0」 → 「1」 に書き換える

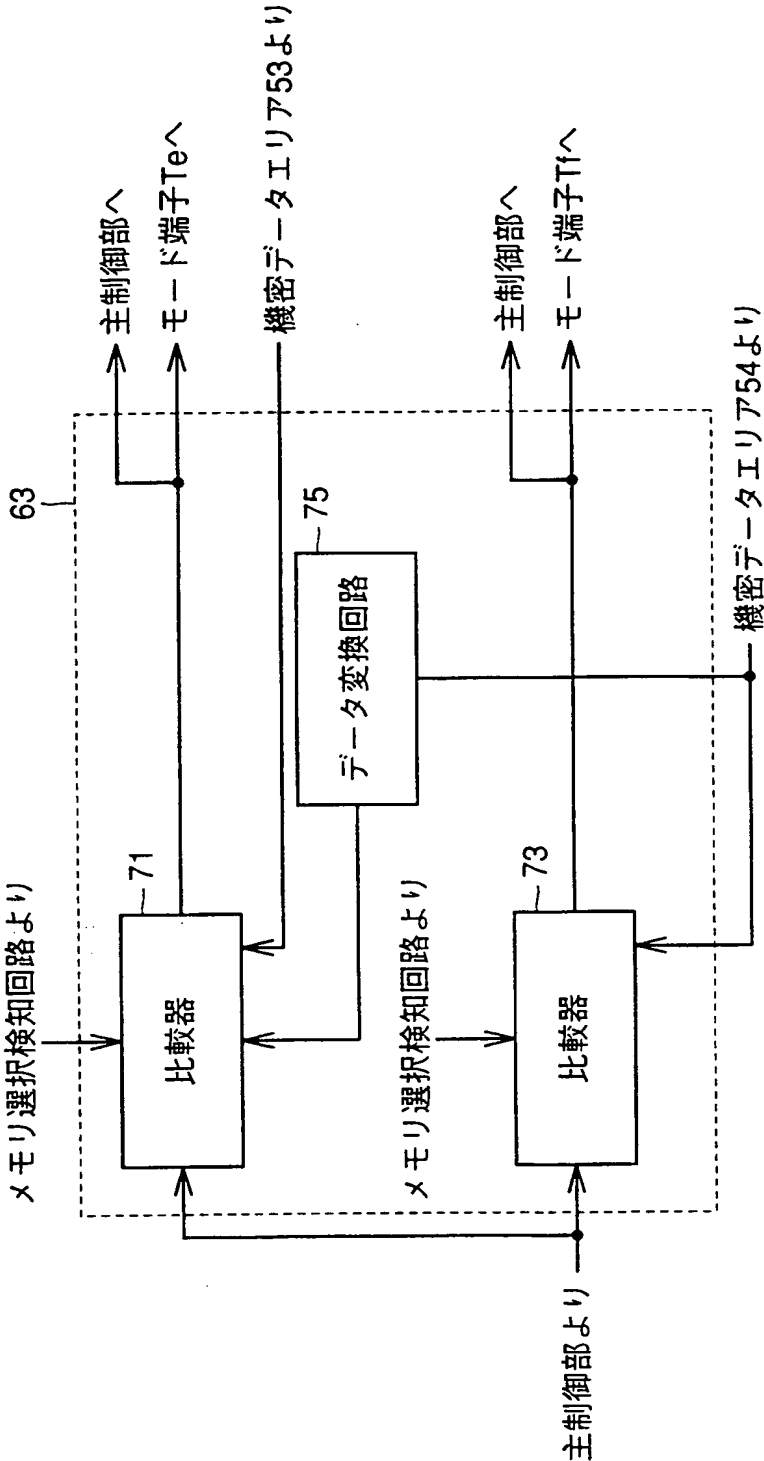
THIS PAGE BLANK (USPTO)

FIG. 6



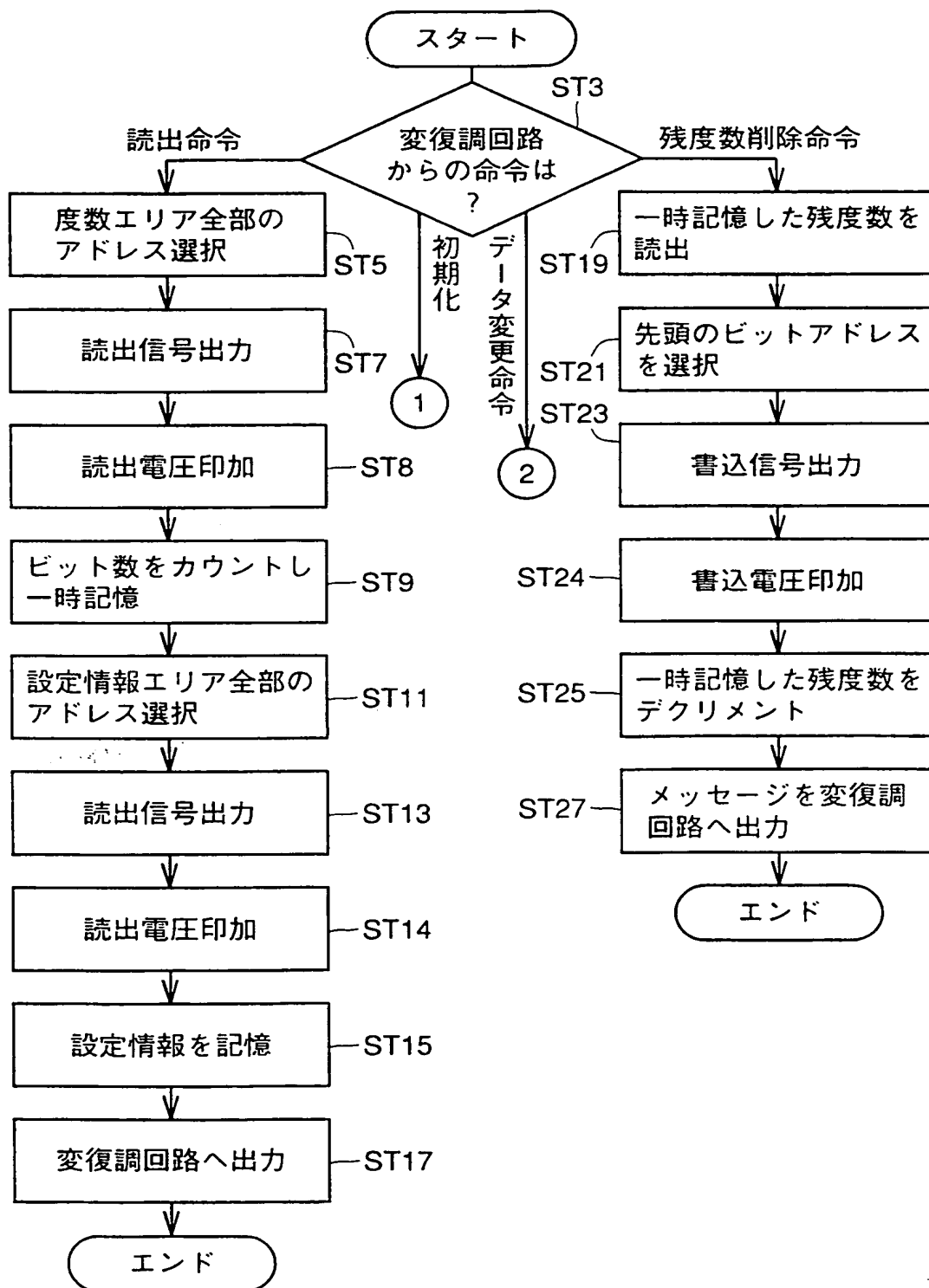
THIS PAGE BLANK (USPTO)

FIG.7



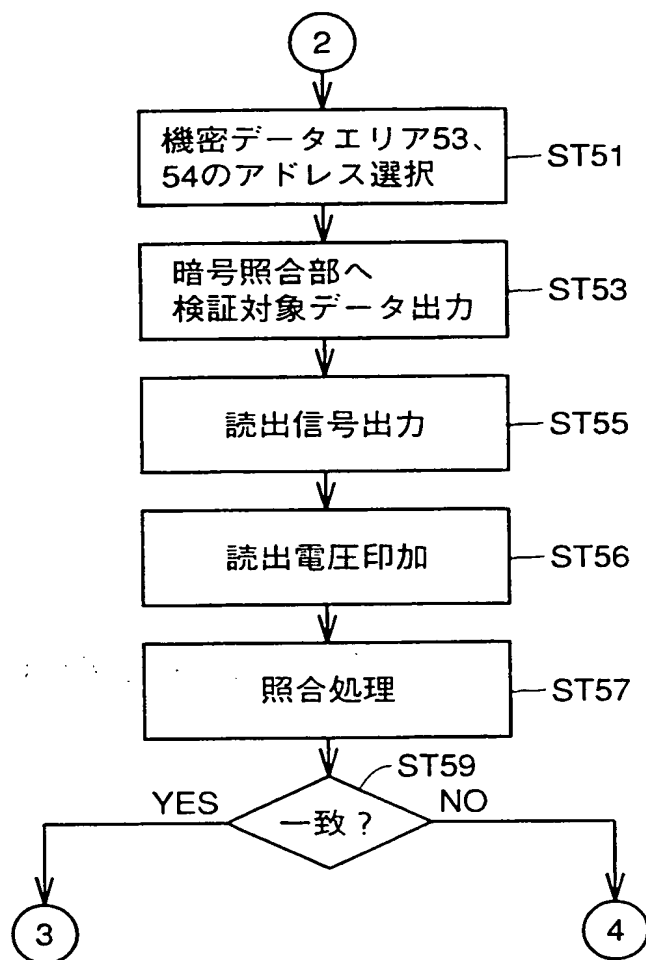
THIS PAGE BLANK (USPTO)

FIG.8



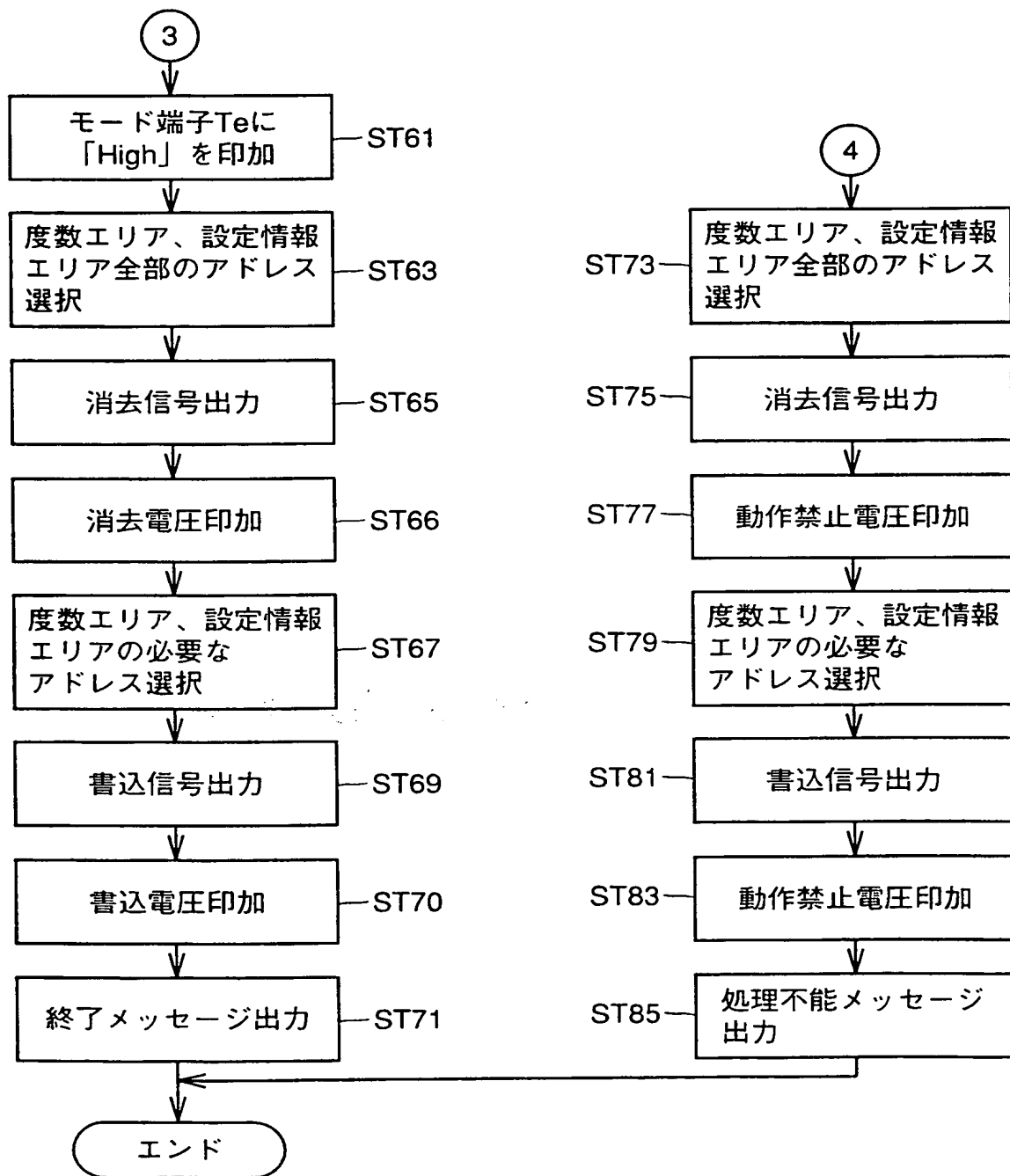
THIS PAGE BLANK (USPTO)

FIG.9



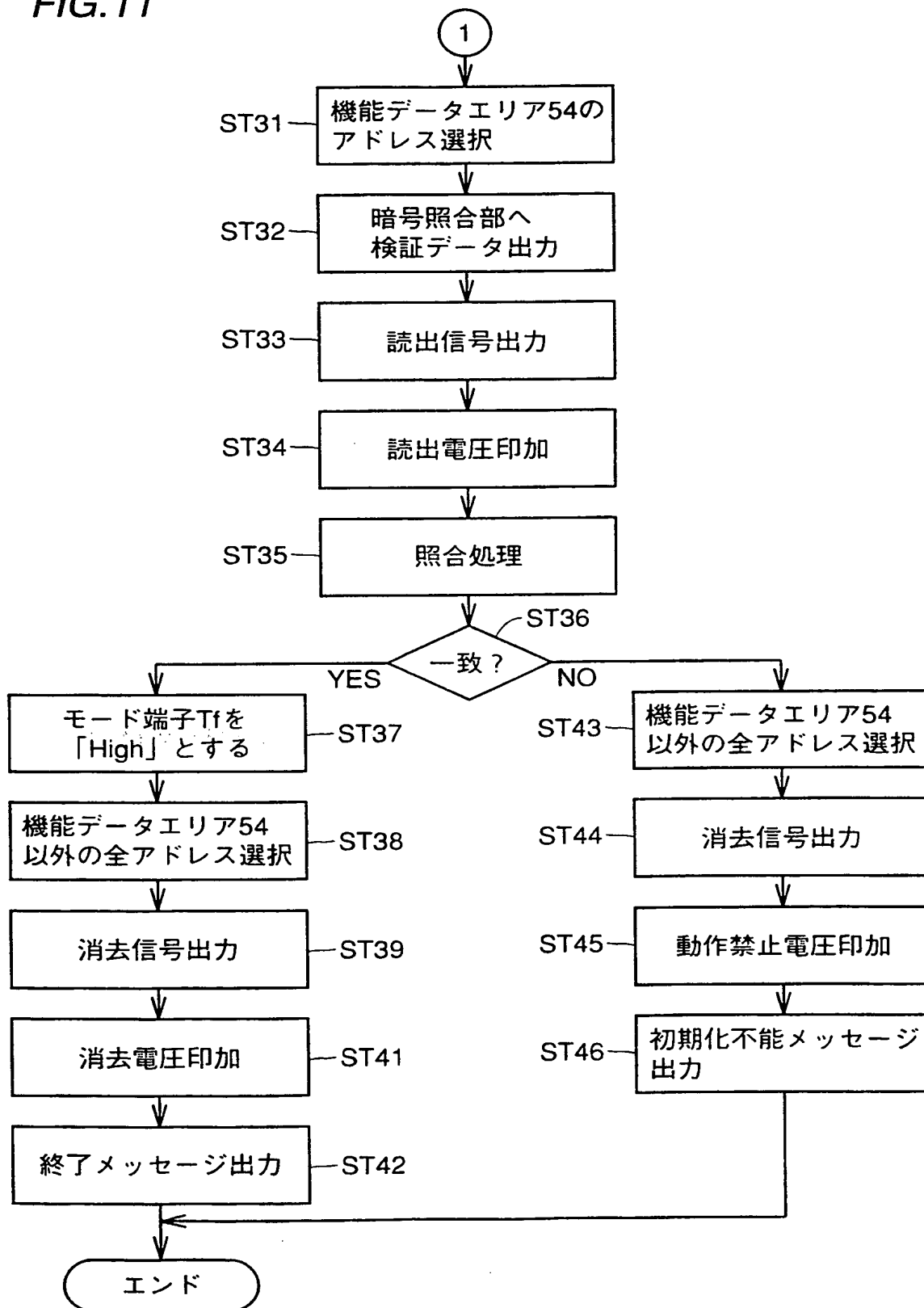
THIS PAGE BLANK (USPTO)

FIG. 10



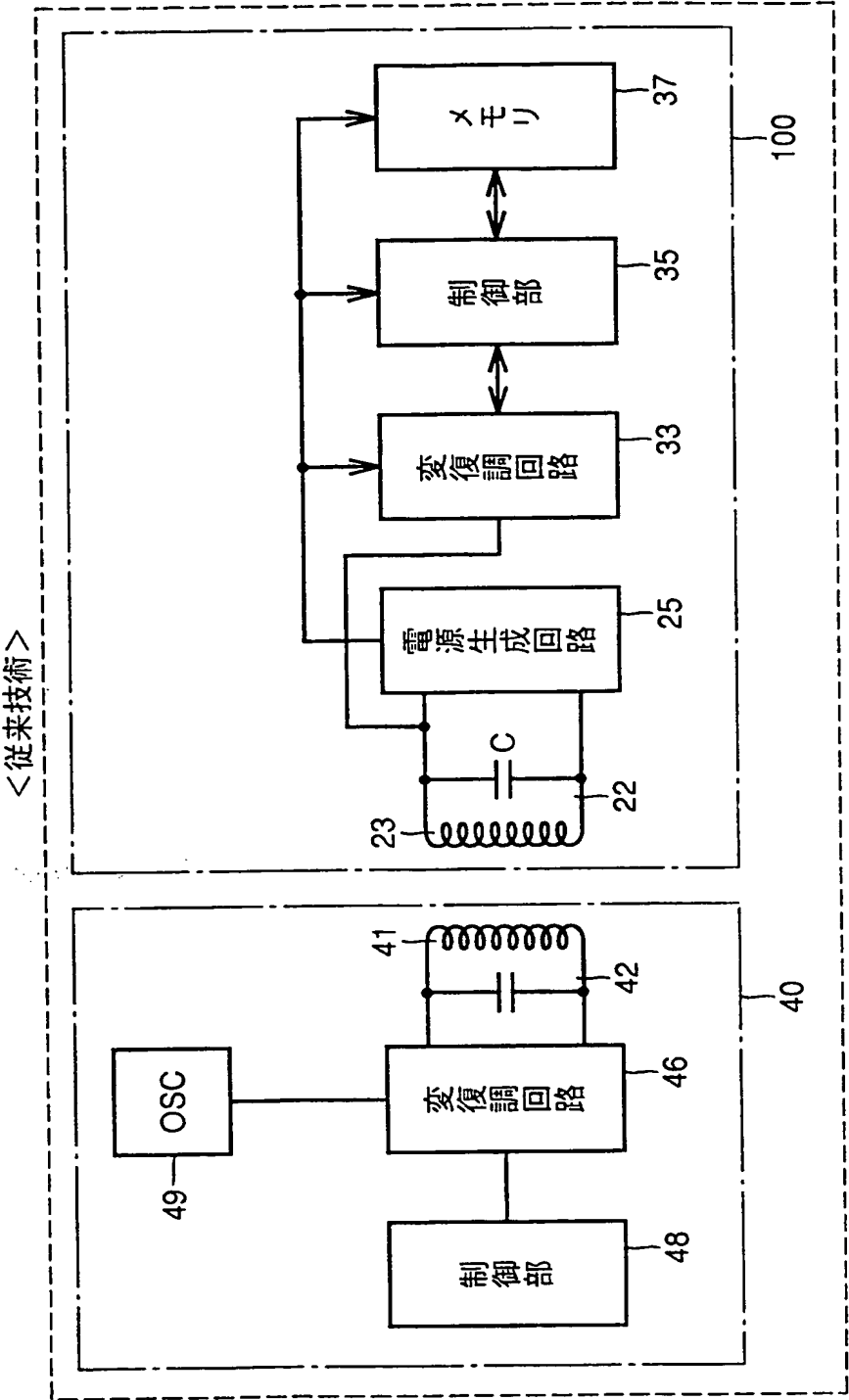
THIS PAGE BLANK (USPTO)

FIG. 11



THIS PAGE BLANK (USPTO)

FIG.12



THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP98/00512

A. CLASSIFICATION OF SUBJECT MATTER
Int.C1⁶ G06K19/073, G07B15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.C1⁶ G06K19/00-19/073, G07B15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1971-1995 Kokai Jitsuyo Shinan Koho 1971-1995
Toroku Jitsuyo Shinan Koho 1994-1998

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP, 7-105335, A (Toppan Printing Co., Ltd.), April 21, 1995 (21. 04. 95), Par. Nos. [0008] to [0010] ; Fig. 1 & EP, 646892, A & AU, 9474346, A & US, 5504701, A	1-10

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
May 7, 1998 (07. 05. 98)

Date of mailing of the international search report
May 19, 1998 (19. 05. 98)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

THIS PAGE BLANK (USPTO)

国際調査報告

国際出願番号 PCT/J P 98/00512

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.⁸ G06K19/073, G07B15/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.⁸ G06K19/00-19/073, G07B15/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1971-1995年
日本国登録実用新案公報	1994-1998年
日本国公開実用新案公報	1971-1995年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	J P, 7-105335, A (凸版印刷株式会社), 21. 4月. 1995 (21. 04. 95), 段落【0008】-【0010】, 図1 & EP, 646892, A&AU, 9474346, A & US, 5504701, A	1-10

☐ C欄の続きにも文献が列举されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

- 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 先行文献ではあるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

- 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

07. 05. 98

国際調査報告の発送日

19.05.98

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

高松 猛

印

5 B

7 6 2 3

電話番号 03-3581-1101 内線 3546

THIS PAGE BLANK (USPTO)